Show Me the Money

By Barry P. Chaiken, MD, MPH

As the country wonders about the next iteration or obliteration of the Affordable Care Act and how to prepare for changes to the healthcare marketplace in 2017, the 1996 movie *Jerry Maguire,* starring Tom Cruise and Cuba Gooding Jr., may have all the answers we need. Cruise plays Maguire, a sports agent who represents Rod Tidwell, a fictional Arizona Cardinals wide receiver played by Gooding.

In one poignant scene, Rod chastises Jerry in an effort to motivate him to secure a higher-value contract for Rod's services to the Cardinals. Through the repetitive mantra "show me the money, Jerry," Rod makes it clear to his agent that only the money value of the contract matters ("Jerry Maguire," 2016).

Wise observers of healthcare trends understand that the industry's direction always relates to the flow of money. Provider organizations, clinicians, life science companies, and healthcare information technology vendors all take positions that closely follow the economic incentives presented by the marketplace. So, to understand the fate of the Affordable Care Act and the focus of the industry in 2017, just ask the various stakeholders to "show you the money."

Affordable Care Act

At the close of 2017, some version of "x-care" will exist. Whether it be Obamacare, Trumpcare, or Ryancare, no one's mantra will be "I don't care." There is just too much money at stake.

The current muted response to the threat of the Affordable Care Act's repeal is mostly due to the various interests figuring out how to position themselves to benefit from changes to the current law. In time, the battle lines will be drawn, and as we hear statements focused on patient access, quality of care, and clinician autonomy, the underlying theme will be the fight to enhance the economic position of the interested party. Similarly, our politicians will be motivated by their reelection prospects, making it unlikely that the 20 million people newly enrolled under the Affordable Care Act will be forced to lose coverage through its indiscriminate repeal.

Value from EMRs

After spending more than $30 billion on incentive payments, many in and out of government wonder what value the investment in electronic medical records (EMR) has delivered to patients. Similarly, many hospital boards of directors, provider organization leadership groups, and physicians in private practice wonder about their return on investment from implementing healthcare information technology (HIT) systems.

EMRs are expensive to implement and maintain, and there is no clear evidence that they increase productivity, enhance quality, or reduce medical errors. Although studies do show some benefits obtained from the use of EMRs, this evidence is not definitive, and any positives from their use are not widely reported across the industry.

To understand our struggle to obtain value from EMRs, it is important to "show you the money." The HITECH Act motivated organizations to purchase EMRs to obtain incentive payments through the federal government's meaningful use program. As deploying an EMR is both expensive and risky, provider organizations focused on implementing EMRs in their most basic format, forgoing the process and clinical workflow redesign necessary to effectively leverage the power of EMRs to strengthen patient care. Organizations most feared a loss of revenue due to suboptimal coding, so they focused on proper clinician documentation to preserve current revenue streams.

EMRs are expensive to implement and maintain, and there is no clear evidence that they increase productivity, enhance quality, or reduce medical errors.

In turn, vendor organizations supported these "generic" implementations as they avoided delays in go-live dates. Accounting rules require software to be installed and functional before revenue from the sale can be recognized; thus, vendors prefer short implementation project plans so they can report the revenue to shareholders, and so executives and sales staff can secure related bonuses or commissions. In summary,

most stakeholders were incented to implement their EMR quickly, putting off the hard work of workflow redesign for another, indeterminate time.

Now that most organizations are finished with their primary EMR deployment, they face the necessary version upgrade, and the associated disruption and expense. Upgrades, which can last from six months to more than a year, offer providers who never took the time to design new workflows a second chance to take advantage of their EMRs' power. Without an effort put into workflow revision, EMRs will not be able to deliver value or a real return on investment; they won't be able to "show you the money."

Cybersecurity

While most of the country focuses on the Russian hacks of our political institutions (Higgins, 2016), leaders at provider organizations need to turn their attention to their own facilities' cybersecurity. Although most IT departments are focused on ransomware and Trojan-carrying email spam, the threats to our HIT are much broader.

The explosion of connected devices that leverage the Internet of Things exponentially expands the number of devices that must be protected from attack. In addition, the vast amount of proprietary code used by these devices, coupled with the lack of widely used security standards for protected health information (PHI), presents an enormous problem for CIOs and their staff tasked to protect HIT infrastructure and its stored PHI.

The healthcare industry has already sprinted to catch up to other industries in the use of IT, and a similar sprint will be needed to proactively address the various cyberthreats. Although ransomware presents a disrupting threat to provider organizations, there are proven approaches to minimize its risks and mitigate its effects. The same applies to data breaches through which criminals steal patient information, mostly for its financial value.

Threats to databases of PHI now expand beyond the theft of items such as Social Security numbers. Invasions of these databases by criminals trained in the dark web can lead to alteration of laboratory values, digital images, and even consultant reports ("Dark web," 2016). The relatively unprotected Internet of Things allows for hacking of connected medical devices and, in turn, corruption of the values stored in EMRs and other HIT repositories. Alteration of clinical results, needless to say, is dangerous for patients. Yet as bad as such a situation sounds, imagine how frightening it would be if a hack allowed an invader to take real-time control of connected medical equipment and sensors during patient care. Are providers prepared to address such high-stakes challenges?

Although some large integrated delivery networks might ante up the resources to protect their institutions from cyberthreats, most smaller hospitals and physician practices are vulnerable and will remain so for some time. As long as there is money to be made in cybercrime, nefarious individuals will work hard to cash in.

In *Jerry Maguire,* Rod taught Jerry an important lesson that we all should learn. To better understand trends and the direction of an industry, first ask yourself "show me the money."

Barry Chaiken *is the president of DocsNetwork Ltd. and has more than 25 years of experience in medical research, epidemiology, clinical information technology, and patient safety. He is board-certified in general preventive medicine and public health and is a fellow, and former board member and chair of HIMSS. At DocsNetwork, Chaiken worked on quality improvement studies, health IT clinical transformation projects, and clinical investigations for the National Institutes of Health, UK National Health Service, and Boston University Medical School. He is currently an adjunct professor of informatics at Boston University's School of Management. Chaiken may be contacted at bchaiken@docsnetwork.com.*

REFERENCES

Dark web (n.d.). In *Wikipedia, the Free Encyclopedia.* Retrieved from https://en.wikipedia.org/wiki/Dark_web

Higgins, A. (2016, December 9). Foes of Russia say child pornography is planted to ruin them. *The New York Times.* Retrieved from https://www.nytimes.com/2016/12/09/world/europe/vladimir-putin-russia-fake-news-hacking-cybersecurity.html

Jerry Maguire (n.d.). In *Wikipedia, the Free Encyclopedia.* Retrieved from https://en.wikipedia.org/wiki/Jerry_Maguire